WinExec

Vulnerable to white space issues in executable or path name. Applications should use the CreateProcess function.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4726 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Process management
Software Context	• Process Management
Location	• winbase.h
Description	The WinExec function runs the specified application. This function is provided only for compatibility with 16-bit versions of Windows. Applications should use the CreateProcess function. The executable name is treated as the first white space-delimited string in lpCmdLine. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces.
APIs	**Function Name** / **Comments** WinExec
Method of Attack	"If a malicious user were to create a Trojan program called "Program.exe" on a system, any program that incorrectly calls WinExec using the Program Files directory will now launch the Trojan instead of the intended application." - MSDN article, "A Great Step Forward in Application Security: Documenting Security Implications of C Runtime and Windows APIs" by Michael howard <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp>
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** When desiring to run a / Use CreateProcess function. / Effective.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	specified application		
	If you must use WinExec for legacy reasons	Make sure the application name is a fully qualified path and wrap each command line element with double quotes.	Effective.

Signature Details	UINT WinExec(LPCSTR lpCmdLine, UINT uCmdShow);

Examples of Incorrect Code	`WinExec("C:\\Program Files\ \MyApp", ...)`
	
	`If a malicious user were to create an application called "Program.exe" on a system, any program that incorrectly calls WinExec using the Program Files directory will run this application instead of the intended application.`
	
	`The executable name is treated as the first white space-delimited string in lpCmdLine. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces.`

Examples of Corrected Code	`To avoid this problem, use CreateProcess rather than WinExec. However, if you must use WinExec for legacy reasons, make sure the application name is enclosed in quotation marks as shown in the example below.`
	
	`WinExec("\"C:\\Program Files\ \MyApp.exe\" -L -S", ...)`

Source References	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp[2] • http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/winexec.asp[3]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows

Languages	• C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com